UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/024,075	12/17/2001	Hideaki Negawa	FUJH 19.264	5423

26304 7590 09/19/2005

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
ELMORE, JOHN E	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/024,075	NEGAWA, HIDEAKI	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-20* is/are rejected.

7)☒ Claim(s) *4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

ET

DETAILED ACTION

1. Claims 1-20 have been examined.

Claim Objections

2. **Claim 8 is objected to** because of the following informalities: the term "said first decryption key" (lines 4, 5 and 7) presumably should read "said first encryption key". Appropriate correction is required.

3. **Claim 16 is objected to** because of the following informalities: the term "that is valid after the updating timing" (lines 27-28) presumably should read "that is valid before the updating timing". Appropriate correction is required.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1, 2, 5, 6, 8, and 10-14 are rejected under 35 U.S.C. 102(e)** as being anticipated by Grimes et al. (2002/0002674), hereafter Grimes.

Regarding claim 1, Grimes discloses a multicast system having a multicast server and a plurality of clients,

said multicast server (NOC 12) comprising:

a data encryption unit for encrypting said data by using a first encryption key (Fig. 3A; para.0045);

a data transmission unit for transmitting said data encrypted by said data encryption unit to said plurality of clients by multicasting (Fig. 3A; para. 0025, 0044 and 0045);

a key encryption unit for encrypting said first encryption using a second encryption key (Fig. 3A; para. 0045 and 0054); and

a key transmission unit for transmitting said first encryption key encrypted by said key encryption unit by unicasting to at least one of the plurality of clients, said at least one client subscribing to said data distribution service (para. 0040); and

said at least one client comprising:

a key reception unit for receiving said encrypted first encryption key transmitted by said transmission unit (Fig. 3B and 5D; para. 0048 and 0056);

a key decryption unit for decrypting said encrypted first encryption key received by said key reception unit, using a decryption key (Fig. 3B and 5D; para. 0048 and 0056); and

a data decryption unit for decrypting the encrypted data transmitted by said data transmission unit, using the first encryption key obtained by said decryption unit (Fig. 3B and 5D; para 0047 and 0056).

Regarding claim 2, Grimes teaches all the limitations of claim 1; and further teaches that said multicast server further comprises a registration unit for registering a

client of the plurality of clients, that wishes to subscribe to said data distribution service (subscription to content distribution service; para. 0038, 0039, and 0040).

Regarding claim 5, Grimes teaches all the limitations of claim 1, and further teaches that said second encryption key and said decryption key are the same key (session key (decryption key) is generated by client and sent to server for use in encrypting content encryption key; para. 0051).

Regarding claim 6, Grimes teaches all the limitations of claim 5, and further teaches that said second encryption key and said decryption key are separately provided in respective clients subscribed to said data distribution service (session key (second encryption key and decryption key) provided separate from data distribution; para. 0051-0053).

Regarding claim 8, Grimes teaches all the limitations of claim 1, and further teaches that said second encryption key is a key that is obtained by said at least one client encrypting said first encryption key using a public key of said multicast server and transmitting said encrypted first encryption key to said multicast server, and said multicast server decrypting said encrypted first encryption key using its own secret key (second encryption key (session key) obtained by client, encrypted using public key of server, and transmitted to server; Fig. 5A; para. 0050 and 0051).

Regarding claim 10, this is a method version of the claimed system above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Regarding claim 11, this is a device version of the claimed system above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Regarding claim 12, this is a method version of the claimed system above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Regarding claim 13, this is a device version of the claimed system above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Regarding claim 14, this is a method version of the claimed system above (claim 1). Therefore, for reasons applied above, such a claim also is anticipated.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claim 3 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Grimes.

Regarding claim 3, Grimes teaches all the limitations of claim 1, but Grimes does not explicitly explain that said multicast server further comprises a charging unit for applying quantity-based charges to said at least one client in accordance with the time or quantity of data received.

However, Grimes teaches that the multicast server (NOC 12) manages the purchase of a pay-per-view ticket and a subscription by a client (para. 0039). One of ordinary skill in the art would recognize that both the pay-per-view fee and the subscription fee is associated with usage time or quantity of data received. Therefore, it would be obvious to one of ordinary skill in the art to provide for a charging unit for

applying quantity-based charges to said at least one client in accordance with the time or quantity of data received for the motivation of facilitating the purchase of a client subscription.

7. **Claim 7 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Grimes in view of Quisquater et al. ("Secure Personalization Using Proxy Cryptography," 2000), hereafter Quisquater.

Regarding claim 7, Grimes teaches all the limitations of claim 5, but does not explicitly explain that said decryption key is constituted of hardware circuitry or a semiconductor chip.

However, it is widely known in the art that a semiconductor chip in the form of a cryptographic coprocessor or a smart card provides a means to generate or store an encryption key. Quisquater, for example, teaches a system for authenticating users wherein a smart card generates and transmits a symmetric key for the purpose of better securing the communication between the client and a server (pages 2-4). One of ordinary skill in the art would recognize that the decryption key (symmetric or session key) used to secure the communication between the client and the multicast server would be generated by the client via a smart card where possession of the smart card serves as a secure authenticating token, particularly where the smart card is preprogrammed by the manufacturer and subsequently purchased by the client.

Therefore, it would be obvious to one of ordinary skill in the art to modify the system of Grimes with the teaching of Quisquater to provide that said decryption key is

constituted of hardware circuitry or a semiconductor chip. One would be motivated to do so in order to provide more secure communication between the client and the multicast server.

8. **Claim 9 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Grimes in view of Schneier ("Applied Cryptography," 1996).

Regarding claim 9, Grimes teaches all the limitations of claim 1, but does not explain that said second encryption key is a public key of a digital certificate issued by the public key infrastructure in respect of a client that has subscribed to said data subscription service, and said decryption key is a secret key of said digital certificate.

However, Schneier teaches a system of secure communications wherein a public key of a digital certificate issued by the public key infrastructure in respect of a client is utilized to send a decryption key (symmetric key) from a server to a client as a secret key of said digital certificate (pages 32-33) for the purpose of more securely transmitting a symmetric key that is used to decrypt data, as the public key algorithm is more secure though slower than the symmetric key algorithm.

Therefore, it would be obvious to one of ordinary skill in the art to modify the system of Grimes with the teaching of Schneier to provide that said second encryption key is a public key of a digital certificate issued by the public key infrastructure in respect of a client that has subscribed to said data subscription service, and said decryption key is a secret key of said digital certificate. One would be motivated to do

so in order to provide more secure transmission of the decryption key between the multicast server and the client.

9. **Claims 15-20 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Grimes in view of McDaniel et al ("Antigone: A Flexible Framework for Secure Group Communications," 1999), hereafter McDaniel, and further in view of Mittra ("Iolus: A Framework for Scalable Secure Multicasting," 1997).

Regarding claim 15, this is a system version of the claimed method below (claim 16). Therefore, for reasons applied below, such a claim also would have been obvious.

Regarding claim 16, Grimes is relied upon for teaching as applied to claim 1, in particular encrypting the data using a data encryption key, transmitting the data to a plurality of clients, and decrypting the encrypted data using the data encryption key. But Grimes does not explain:

updating the data encryption key, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing in said multicast server, said data encryption key that is valid after the updating timing being in a relationship that is obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

encrypting said updating key corresponding to the data encryption key that is valid after the updating timing by using the data encryption key that is valid after the

updating timing at intervals of said updating timing, and transmitting the encrypted updating key to said at least one client by unicasting or multicasting in said multicast server;

decrypting the encrypted updating key by using a currently valid data decryption key on receiving the encrypted updating key transmitted from said multicasting server in said at least one client; and

updating a data decryption key that is valid before the updating timing to a data decryption key that is valid after the updating timing at intervals of the updating timing in said at least one client, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating time to said data decryption key that is valid before the updating timing at said intervals, a data decryption key on subscribing to said data distribution service being given from outside.

However, McDaniel teaches a method of rekeying a multicast group key involving updating the data encryption key (group session key), at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing (new group session key) in said multicast server for the purpose of increasing security by using the encryption key only for a limited time in order to discourage cryptoanalysis (time-sensitive rekeying policy; page 3).

And Mittra teaches a method of rekeying a multicast group key over periodic time intervals involving encrypting a new group key by using the at intervals of said updating timing, and transmitting the encrypted updating key to clients by unicasting or

multicasting in a multicast server for the purpose of providing a simple and secure means of distributing the new group key (pages 7-8, section 6.6). One of ordinary skill in the art would recognize that the new group key is equivalent to the updating key corresponding to the data encryption key that is valid after the updating timing and that the old group key is equivalent to the data encryption key that is valid after the updating timing. One of ordinary skill also would recognize that where an encrypted updating key is transmitted to a client, the encrypted updating key subsequently must be decrypted using the currently valid data decryption key (old group key).

Further, one of ordinary skill in the art would recognize that the method of generating a new data decryption key, which is valid after the updating timing, by applying an updating key to the prior data decryption key, which is valid before the updating timing, at the client is functionally equivalent to generating the new data encryption key at the multicast server and transmitting the new data encryption key to the client (to replace the prior data decryption key) because the same updating key is applied to the same symmetric key whether at the client or the multicast server; that is, the same mathematical function is performed.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Grimes with the teaching of McDaniel and Mittra to provide for:

updating the data encryption key, at intervals of a prescribed updating timing, to a data encryption key that is valid after the updating timing in said multicast server, said data encryption key that is valid after the updating timing being in a relationship that is

obtained by applying an updating key corresponding to a data encryption key that is valid before the updating timing to the data encryption key that is valid before the updating timing;

encrypting said updating key corresponding to the data encryption key that is valid after the updating timing by using the data encryption key that is valid after the updating timing at intervals of said updating timing, and transmitting the encrypted updating key to said at least one client by unicasting or multicasting in said multicast server;

decrypting the encrypted updating key by using a currently valid data decryption key on receiving the encrypted updating key transmitted from said multicasting server in said at least one client; and

updating a data decryption key that is valid before the updating timing to a data decryption key that is valid after the updating timing at intervals of the updating timing in said at least one client, said data decryption key that is valid after the updating timing being generated by applying an updating key obtained by decryption using a data decryption key that is valid before the updating time to said data decryption key that is valid before the updating timing at said intervals, a data decryption key on subscribing to said data distribution service being given from outside.

One would be motivated to do so in order to increasing security by using the data encryption key only for a limited time in order to discourage cryptoanalysis and to provide a simple and secure means of updating and distributing the data encryption/decryption keys.

Regarding claims 17-19, these are device versions of the claimed method above (claim 16). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claims 18 and 20, these are other method versions of the claimed method above (claim 16). Therefore, for reasons applied above, such a claim also would have been obvious.

Allowable Subject Matter

10. **Claim 4 is objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Regarding claim 4, the closest prior art, Grimes, teaches all the limitations of claim 2, but does not explicitly explain that said multicast server further comprises a deletion data reception unit for receiving deletion data indicating that the client registered by said registration unit has been deleted at least said first encryption key held by said client itself, said deletion data being transmitted from said client; and an erasure unit for erasing from said registration unit the client that has transmitted said deletion data, when said deletion data reception unit receives said deletion data; and that said client further comprises a deletion unit for deleting at least said first encryption key held by said client itself in the event of withdrawal from said data distribution

service; and a deletion data transmission unit for generating said deletion data and transmitting said deletion data to said multicast server.

Grimes does not directly address the cancellation of a subscription, but teaches in the preferred embodiment that the multicast content is accessed by retrieving a decryption key from the multicast server for every session of usage, as the decryption key is encrypted in part using a session key (para. 0055). Hence, Grimes provides no suggestion that the system comprises a deletion data reception unit, a deletion unit, or a deletion data transmission unit.

While it is widely known in the art that digital rights management systems erase from the client encrypted content and/or its associated key(s) used to decrypt the content upon cancellation or expiration of a subscription, the prior art does not appear to address the means whereby the client initiates the cancellation of a subscription by erasing at least the key used to decrypt the content.

Therefore, it would not seem obvious to modify the system of Grimes to provide for a deletion data reception unit, a deletion unit, or a deletion data transmission unit.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100